HIPAA - Privacy – Business Associates

TRICARE Management Activity, Electronic Business Policy & Standards

January 2003

OSD(HA), TMA eBPS

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

Highlights

General Requirement

By law, the Privacy Rule applies only to health plans, health care clearinghouses, and certain health care providers. In today's health care system, however, most health care providers and health plans do not carry out all of their health care activities and functions by themselves; they require assistance from a variety of contractors and other businesses. In allowing providers and plans to give protected health information (PHI) to these "business associates," the Privacy Rule conditions such disclosures on the provider or plan obtaining, typically by contract, satisfactory assurances that the business associate will use the information only for the purposes for which they were engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with the covered entity's duties to provide individuals with access to health information about them and a history of certain disclosures. For example, if the business associate maintains the only copy of information, it must promise to cooperate with the covered entity to provide individuals access to information upon request. PHI may be disclosed to a business associate *only* to help the providers and plans carry out their health care functions - not for independent use by the business associate.

"Business Associate" Defined

What is a "business associate?"

- A business associate is a person or entity who provides certain functions, activities, or services for or to a covered entity, involving the use and/or disclosure of PHI
- A business associate is not a member of the health care provider, health plan, or other covered entity's workforce
- A health care provider, health plan, or other covered entity can also be a business associate to another covered entity
- The rule includes exceptions. The business associate requirements do not apply to covered entities who disclose PHI to providers for treatment purposes - for example, information exchanges between a hospital and physicians with admitting privileges at the hospital

Business Associates' Compliance with the Privacy Rule

The Privacy Rule does not "pass through" its requirements to business associates or otherwise cause business associates to comply with the terms of the rule. The assurances that covered entities must obtain prior to disclosing PHI to business associates create a set of contractual obligations far narrower than the provisions of the rule, to protect information generally and help the covered entity comply with its obligations under the rule. For example, covered entities do not need to ask their business associates to agree to appoint a privacy officer, or develop policies and procedures for use and disclosure of PHI.

HIPAA PROGRAM OFFICE

Skyline 5, Suite 810
5111 Leesburg Pike
Falls Church, VA
22041-3206
Ph: 703-681-5611
Fax: 703-681-8845

TMA HIPAA Website:
www.tricare.osd.mil/hipaa

E-Mail:
hipaamail@tma.osd.mil

TRICARE Management Activity

Privacy Violations by Business Associates and Liability

A health care provider, health plan, or other covered entity is not liable for privacy violations of a business associate. Covered entities are not required to actively monitor or oversee the means by which the business associate carries out safeguards or the extent to which the business associate abides by the requirements of the contract.

Moreover, a business associate's violation of the terms of the contract does not, in and of itself, constitute a violation of the rule by the covered entity. The contract must obligate the business associate to advise the covered entity when violations have occurred.

If the covered entity becomes aware of a pattern or practice of the business associate that constitutes a material breach or violation of the business associate's obligations under its contract, the covered entity must take "reasonable steps" to cure the breach or to end the violation. Reasonable steps will vary with the circumstances and nature of the business relationship.

If such steps are not successful, the covered entity must terminate the contract if feasible. The rule also provides for circumstances in which termination is not feasible, for example, where there are no other viable business alternatives for the covered entity. In such circumstances where termination is not feasible, the covered entity must report the problem to the Department of Health and Human Services. All such reports from components of the Military Health System (MHS) shall be forwarded to the TRICARE Management Activity.

Only if the covered entity fails to take the kinds of steps described above would it be considered to be out of compliance with the requirements of the rule.

Privacy Contract Requirements

At a minimum, the covered entity's contract with a business associate should contain specific language in the following areas in order to comply with the Privacy Rule:

- Use of PHI
- Appropriate plan to safeguard PHI
- Disclosure to third parties, if applicable
- Accounting for disclosure of PHI
- Plan for reporting of privacy violations by a business associate
- Destruction or return of PHI upon termination of the contract, or, where it is not feasible to destroy the PHI, the continuance indefinitely of the privacy component of the contract

A business associate contract language clause is available at www.tricare.osd.mil/hipaa.